REMARKS

In accordance with the foregoing, the specification and claims have not been amended. No claims have been cancelled. Claims 1-15 are pending and under consideration.

Favorable reconsideration of this application, in light of the following discussion is respectfully requested.

REJECTION UNDER 35 U.S.C. § 102(e)

Claims 1-12 were rejected under 35 U.S.C. § 102(e) as unpatentable over Yup et al (U.S. Pat. No. 6,937,727). This rejection is respectfully traversed because Yup does not teach or suggest all of the limitations recited at least in independent claim 1.

"Anticipation requires the presence in a single prior art reference the disclosure of each and every element of the claimed invention, arranged as in the claim." Lindemann Maschinenfabrik GMBH v. American Hoise and Derrick Co., 221 USPQ 481, 485 (Fed. Cir 1984). The Patent Office has the burden of making out a prima facie case, which requires it to produce the factual basis for its rejection in an application under §§102 and 103. In re Warner, 154 USPQ 173, 177 (CCPA 1967).

The present invention discloses a circuit configuration that allows for a reduced circuit size while enabling high-speed processing for implementing an AES block cipher algorithm. Significant features of the invention include, but are not limited to, an intermediate register and a shift row transformation circuit that are commonly used. Additionally, the shift row transformation is only executed using a processing block length while other processes are executed using an execution block length. There is also included a second selector that selectively outputs a value from among a first selector, an intermediate register, a shift row transformation circuit, a Byte Sub transformation circuit, or a Mix Column transformation circuit. These features of the invention can be seen, for example, by an embodiment illustrated in Figure 4 of the present application.

Claim 1 recites "a first selector that segments input data into execution block lengths smaller than said processing block length." Yup does not disclose or suggest this feature. In rejecting claim 1, the Examiner cites column 1, line 16 to column 2, line 46 in Yup to show this limitation. These sections of Yup merely describe the generic AES block cipher algorithm. There is no specific structure or particular implementation of the algorithm disclosed in these sections, especially the explicit structure recited in claim 1 and described for the present invention.

Additionally, the remaining disclosure of Yup does not teach or suggest these claimed features for the invention. In the present invention, an input register receives and temporarily stores input data. The input data block size is larger than the size of the data that is processed. For this reason, a first selector selects a 32-bit data block from this input register. This 32-bit data block is then inputted into the first Round Key Addition circuit for processing. In contrast, Yup shows input registers, which are preferably first-in-first-out registers, that receive a data string, preferably 64-bits in length (Yup, column 4, lines 50-55). These input registers then input data into a buffer register until a predetermined data block is stored, which is larger than the input buffer size (Yup, column 4, line 64 to column 5, line 5). This entire data block from the buffer register is then used in various logical operations and the first AddRoundKey function (column 5 lines 6-34, column 5 lines 2-15). This shows that the entire input buffer of Yup, which is preferably at least 128-bits, is used in the AES functional block. In contrast with the present invention, Yup shows adding various data blocks into a buffer then performing various operations on the entire summation of input data blocks. Therefore, Yup does not disclose an input value divided into an execution block length at a first selector. The present invention, as recited in claim 1, requires that a first selector segment the input data into smaller block lengths than the initial input data. As such, Yup does not disclose or suggest "a first selector that segments input data into execution block lengths smaller than said processing block length."

Claim 1 also recites "a second selector that outputs to said first Round Key Addition circuit one output from among the outputs of said first selector, intermediate register/Shift Row transformation circuit, Byte Sub transformation circuit, or Mix column transformation circuit." Yup neither teaches nor suggests this claimed limitation. As stated above, in the Office Action rejection of claim 1, the Examiner cites column 1, line 16 to column 2, line 46 in Yup to show this claimed limitation. These sections of Yup merely describe the generic AES block cipher algorithm. There is no discussion to the particular configuration of implementing the AES block cipher algorithm as recited in claim 1 and as described for the present invention.

Additionally, the remaining disclosure of Yup does not teach or suggest the claimed limitation. The present invention shows that the second selector receives input data from the first selector, the ByteSub transformation circuit, the MixColumn transformation circuit, or the intermediate register/Shift Row transformation circuit. Depending on the current processing round, the second selector is set to a different position and sends one of the above listed input values to the first Round Key Addition circuit. Yup does not remotely show the presence of a second selector. As discussed above, Yup does not suggest or disclose a first selector, let alone a second selector for sending various inputs to the first Round Key Addition circuit.

Furthermore, Yup shows a circuit in which a first AddRoundKey 116, an input register 120, a ByteSub/InvByteSub 122, a ShiftRow/InvShiftRow 124, a MixCol/InvMixCol 126, and a second AddRoundKey 118 are connected in series (see Yup, figure 1). Because of this configuration, only the value of the second AddRoundKey 118 is stored in a storage register 110. Therefore, because of the series connection and lack of individual outputs of the ByteSub circuit 122, ShiftRow circuit 124, and the MixCol circuit 126, these individual circuits cannot provide an independent input value to the second selector even if it existed in the disclosure of Yup. The invention of claim 1 indicates individual values being inputted into the second selector. As such, Yup fails to suggest or disclose "a second selector that outputs to said first Round Key Addition circuit one output from among the outputs of said first selector, intermediate register/Shift Row transformation circuit, Byte Sub transformation circuit, or Mix column transformation circuit."

Claim 1 further recites "an intermediate register/Shift Row transformation circuit that temporarily stores the output of said first Round Key Addition circuit and executes Shift Row transformation using said processing block length." Yup neither teaches nor suggests this feature. As stated above, in the Office Action rejection of claim 1, the Examiner cites column 1, line 16 to column 2, line 46 in Yup to show this claim limitation. These sections of Yup merely describe the generic AES block cipher algorithm. There is no discussion to the particular configuration of implementing the AES block cipher algorithm as recited in claim 1 and as described for the present invention.

Additionally, the remaining disclosure of Yup does not teach or suggest the claimed limitation. Contrary to the present invention, Yup states that after the "initial transformation round, the data block is fed back to the cipher block input register 120 for the next transformation round" (Yup, column 6, lines 34-36). As such, Yup does not show an intermediate register that stores a value from the first Round Key Addition. Also, even though Yup discloses a storage register 110, this register is serially connected to the second Round Key Addition circuit. Therefore, it cannot receive the value from the first Round Key Addition circuit. The storage register of Yup also has no ability to perform Shift Row transformations, as recited in claim 1. As such, Yup fails to disclose "an intermediate register/Shift Row transformation circuit that temporarily stores the output of said first Round Key Addition circuit and executes Shift Row transformation using said processing block length."

Because Yup does not disclose each limitation of claim 1, as discussed above, it is respectfully submitted that claim 1 is patentable over the prior art. Claims 2-15 depend, directly

or indirectly, from claim 1 and include all of the features of that claim plus additional features which distinguish over the prior art. Therefore, it is submitted that claims 2-15 are patentably distinguishable over the prior art. It is duly noted that in the Office Action, at page 7, item 16, claims 13-15 were already indicated as containing allowable subject matter. However, in view of the clearly patentable and allowable subject matter of independent claim 1 as noted above, no further modifications to claims 13-15 are considered necessary.

CONCLUSION

In accordance with the foregoing, it is respectfully submitted that all outstanding objections and rejections have been overcome and/or rendered moot. And further, it is respectfully submitted that all pending claims patentably distinguish over the prior art. Thus, there being no further outstanding objections or rejections, the application is submitted as being in condition for allowance which action is earnestly solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 19, 2006

By: David M. Pitcher

David M. Pitcher
Registration No. 25,908

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501